



## UNITED STATES PATENT AND TRADEMARK OFFICE

2  
4  
UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/852,262	05/10/2001	Keith Alexander Harrison	1509-172	5459

7590 09/21/2004

IP Administration  
C/o Hewlett-Packard Company  
3404 East Harmony Road  
Mail Stop 35  
Ft.Collins, CO 80528-9599

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/852,262	HARRISON ET AL.
	Examiner Ellen C Tran	Art Unit 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 10 May 2001.
- 2a) This action is **FINAL**.                            2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-24 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-24 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.
 

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date: _____
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>5/10/01</u> .	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

***DETAILED ACTION***

1. This action is responsive to communication: original application filed 10 May 2001, with acknowledgement of foreign application date of 31 May 2000.
2. Acknowledgement of Pre-Amendment filed 10 May 2001 that modifies the claims.
3. Claims 1-24 are currently pending in this application. Claims 1, 22, 23, and 24 are independent claims.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5. **Claims 1-5, 10, 15-17, and 22-24** are rejected under 35 U.S.C. 102(e) as being anticipated by Lin et al. U.S. Patent No. 6,052,785 (hereinafter '785).

**As to independent claim 1, “A distributed storage system for storing at least one credential, provided by an issuing authority and relating to an identity, the system comprising: at least one unique identity having a local store, the store of the at least one identity securely storing one or more credentials relating to the owner of the identity” is taught in '785 col. 3, lines 41-63;**

**“and a security certificate provided at each identity for ensuring the authenticity of the one or more credentials, the security certificate providing a secure reference to the**

**issuer of the one or more credentials that can be used in verifying the origin of each credential**" is shown in '785 col. 6, lines 37-55.

**As to dependent claim 2, "wherein the at least one identity comprises a hierarchical structure"** is disclosed in '785 col. 9, lines 1-16.

**As to dependent claim 3, "wherein the at least one identity comprises at least one role, the role being a subset of the identity having its own credentials within the identity"** is taught in '785 col. 9, lines 1-16.

**As to dependent claim 4, "further comprising a host site, the host site having a plurality of identities and associated stores"** is shown in '785 col. 3, lines 40-51.

**As to dependent claim 5, "wherein the host site comprises a management module for managing data access to and from the each of the identities and their associated stores"** is disclosed in '785 col. 3, lines 40-51.

**As to dependent claim 10, "wherein the identity is arranged to store a private key of the identity for encryption of the identity"** is taught in '785 col. 6, lines 8-23.

**As to dependent claim 15, "wherein at least some of the credentials are arranged to be encrypted"** is taught in '785 col. 5, line 64 through col. 6, line 8.

**As to dependent claim 16, "wherein the one or more credentials each refer to the corresponding security certificate"** is shown in '785 col. 6, lines 37-55.

**As to dependent claim 17, "wherein the security certificate comprises information describing the issuer, the identity to whom the certificate has been issued, a validity period and a list of credentials to which the certificate relates"** is disclosed in '785 col. 7, lines 19-41.

**As to independent claim 22, “A method of storing credentials relating to identities provided by an issuing authority in a distributed manner, the method comprising: securely storing one or more credentials relating to the owner of an identity in a local store of the identity; and providing a security certificate at the identity for ensuring the authenticity of the one or more credentials”** is taught in ‘785 col. 3, lines 41-63;

**“the security certificate providing a secure reference to the issuer of the one or more credentials that can be used in verifying origin of each credential”** is shown in ‘785 col. 6, lines 37-55.

**As to independent claim 23, “An identity of an entity for making available credentials belonging to the entity to other entities, the identity comprising: a local store arranged to securely hold one or more credentials relating to the entity; and a certificate processing module for reading and verifying received security certificates and creating security certificates for transmission”** is taught in ‘785 col. 3, lines 41-63;

**“the security certificates providing a secure reference to the issuer of the one or more credentials that can be used in verifying the origin of each credential”** is shown in ‘785 col. 6, lines 37-55.

**As to independent claim 24, “A distributed storage system for storing a plurality of credentials, the system comprising a plurality of identities for making available credentials belonging to an entity to other entities, each entity comprising a local store arranged to securely hold one or more credentials relating to the entity; and a certificate processing module for reading and verifying received security certificates and creating security certificates for transmission”** is taught in ‘785 col. 3, lines 41-63;

**“the security certificates providing a secure reference to the issuer of the one or more credentials that can be used in verifying the origin of each credential”** is shown in ‘785 col. 6, lines 37-55.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 6-8, 11-14, 18, 20, and 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘785 in further view of Kausik et al. U.S. Patent No. 6,263,446 (hereinafter ‘446).

**As to dependent claim 6,** the following is not taught in ‘785 “**wherein the host site comprises a trusted financial institution's website**” however ‘446 teaches “We now describe various exemplary embodiments of the invention using the exemplary context of a user operating a web browser ... Those skilled in the art will recognize that the invention is applicable to other client-server environments as well, including but not limited to databases, medical client stations, and financial trading stations” in col. 3, lines 10-21.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of ‘785 that shown a credential manager to include the capability to provide credentials for financial institutions. One of ordinary skill in the art would have been

motivated to perform such a modification to protect information of high value. As indicated by '446 (see col. 1, lines 11 et seq.) "In networked computer deployments, users of client computers are required to authenticate themselves to server computers for applications such as electronic mail, accessing privileged or confidential information, purchasing goods or services, and many other electronic commerce transactions. When the information involved is of relatively low value, it may be sufficient for the user to authenticate himself with a simple password. However, when the information is of high value, or when the data network is unsecured, simple passwords are insufficient to control access effectively".

**As to dependent claim 7, "wherein the identity or host site comprises a website"** is shown in '446 col. 3, lines 22-42 "Referring now to FIG. 1, a user at Browser 140 wishes to access a Web Server 110 to conduct an electronic transaction. Web Server 110 is, in turn, safeguarded by Access Control Server 120, which prevents unauthorized access to Transaction Server 130. For example, Web Server 110 might be a company's home page, Access Control Server 120 might be a firewall, and Transaction Server 130 might contain proprietary company data that the user wishes to access".

**As to dependent claim 8, "wherein the identity further comprises a homepage for providing general information regarding the identity"** is disclosed in '446 col. 3, lines 60-67 "The present invention provides a method and apparatus for providing the authentication credential, on demand, to a user who wishes to be able to access servers 110, 120 and/or 130 from a variety of Browsers 140 (the so-called "roaming user")".

**As to dependent claim 11, “wherein the identity is arranged to store a public key of the identity for decryption of the identity”** is shown in ‘446 col. 4, lines 48-59 “The foregoing illustrates the use of so-called shared secrets, whereby the user and the server both share copies of information required to access the system … As a simple example, the user's private key itself could be used in this fashion, for a verifier need only know the corresponding public key to verify the private key”

**As to dependent claim 12, “wherein the public key of the identity is embedded within each credential of the identity”** is disclosed in ‘446 col. 7, lines 6-10 “For greater security, the wallet could be downloaded to the user in camouflaged form, with the decamouflaging occurring at the user's computer. For still greater security, a one-to-one or many-to-one hash process could replace the simple shared secret for the initial server access”.

**As to dependent claim 13, “wherein the identity is arranged to store a public key of the authority which has issued the one or more credentials to the identity”** is taught in 446 col. 4, lines 1-13 “This on-demand roaming capability is provided by a Credential Server 160 that downloads the authentication credential (e.g., private key) to the user at Browser 140 via a software Wallet 150. As used herein, Wallet 150 need only serve as a basic container for the authentication credential. As such, it could be considered to be simply the data structure in which the authentication credential is embodied, or it could be a more sophisticated container having the capability to handle other user-owned items such as a digital certificate or digital currency (including, without limitation, electronic cash or scrip). In a basic embodiment of the invention, Credential Server 160 is embodied as a web server”.

**As to dependent claim 14, “wherein the public keys for each of the at least one role and the identity are stored in the appropriate store or identity”** is shown in ‘446 col. 4, lines 1-13.

**As to dependent claim 18, “wherein the certificate is digitally signed using a private key and the certificate contains the public key (58) for reading the digital signature”** is taught in ‘446 col. 3, lines 43-59 “Before accessing the Transaction Server 130 to perform the electronic transaction, the user first needs to authenticate himself to Access Control Server 120. As mentioned in the Background of the Invention, the user typically authenticates himself by using his private key to perform a cryptographic operation on a challenge sent by the Access Control Server 120. This cryptographic operation might be a simple encryption, a hash followed by encryption (commonly referred to as a digital signature), or still other protocols that are well known to those skilled in the art”.

**As to dependent claim 20, “wherein the identity further comprises a mailbox for receiving messages from other identities”** is taught in ‘446 col. 3, lines 38-42 “Similarly, the electronic transaction may be of virtually any type including, but not limited to, secure electronic mail, accessing privileged or confidential information, and purchasing electronic or physical goods or services”.

**As to dependent claim 21, “wherein the identity further comprises an authorization function module arranged to check that a request for access to the mailbox has originated from an authorized identity”** is shown in ‘446 col. 3, lines 43-49 “Before accessing the Transaction Server 130 to perform the electronic transaction, the user first needs to authenticate himself to Access Control Server 120. As mentioned in the Background of the Invention, the

user typically authenticates himself by using his private key to perform a cryptographic operation on a challenge sent by the Access Control Server”.

8. **Claims 9 and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over '785 in further view of '446 in further view of Liao et al. U.S. Patent No. 6,606,663 (hereinafter '663).

**As to dependent claim 9**, the following is not taught in the combination of teaching from '785 and '446 “**wherein the local store of the identity comprises a portable mobile device which is connectable to a telecommunications network**” however '663 teaches “Referenced by 106 is one of the two-way interactive communication devices that can be a mobile device, ... The base station controls radio or telecommunication links with the mobile devices” in col. 4, lines 12-55.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combination of teachings from '785 and '446 that shown a credential manager with the capability to provide credentials for financial institutions to include the ability to use wireless devices. One of ordinary skill in the art would have been motivated to perform such a modification to enable the use of wireless devices in application that need credentials to be exchanged. As indicated by '663 (see col. 2, lines 3 et seq.) “In a wireless environment, the user agent (a thin client or micro browser) exists on a wireless client device such as a cellular phone ... Since the basic authentication systems defined in RFC2068 requires the credentials to be continually passed with each request, the basic authentication system is not efficient for the wireless environment”.

**As to dependent claim 19, “wherein the identity further comprises a generator module for generating a certificate regarding the identity for use in proxying credentials**

**to the store of a different identity**" is taught in '663 col. 8, lines 1-24 "If the URL belongs to a known protect realm that the proxy server has a credential for, then the proxy server attaches the credential for that realm to the request and the request is forwarded to the Internet server ... the present invention reduces the amount of memory used within each wireless client device since the wireless user agent does not have to implement the mechanism for saving the credentials nor store the credentials ... Finally, the present invention relieves the user from entering the credentials over and over again"

### ***Conclusion***

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Carter	U.S. Patent No. 6,119,230	issued 09/12/2000
Lloyd et al.	U.S. Patent No. 6,219,790	issued 04/17/2001
Luckenbaugh et al.	U.S. Patent No. 6,311,269	issued 10/30/2001

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. **"After 26 October 2004, the examiner can be reach at (571) 272-3842".**

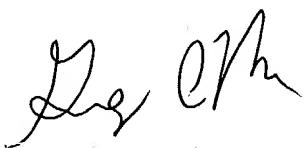
The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran  
Patent Examiner  
Technology Center 2134  
16 September 2004



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100